(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
6 novembre 2003 (06.11.2003)

PCT

(10) Numéro de publication internationale
WO 03/092219 A1

(51) Classification internationale des brevets[7] : H04L 9/06

(21) Numéro de la demande internationale :
PCT/FR03/01190

(22) Date de dépôt international : 15 avril 2003 (15.04.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/05028 23 avril 2002 (23.04.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **SCM MICROSYSTEMS GMBH** [DE/FR]; ZE Athelia II, 216, avenue du Serpolet (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **LOISEL, Yann** [FR/FR]; Office Méditerranéen de Brevets d'Invention et de Marques, Cabinet Hautier, 24, rue Masséna, F-06000 NICE (FR).

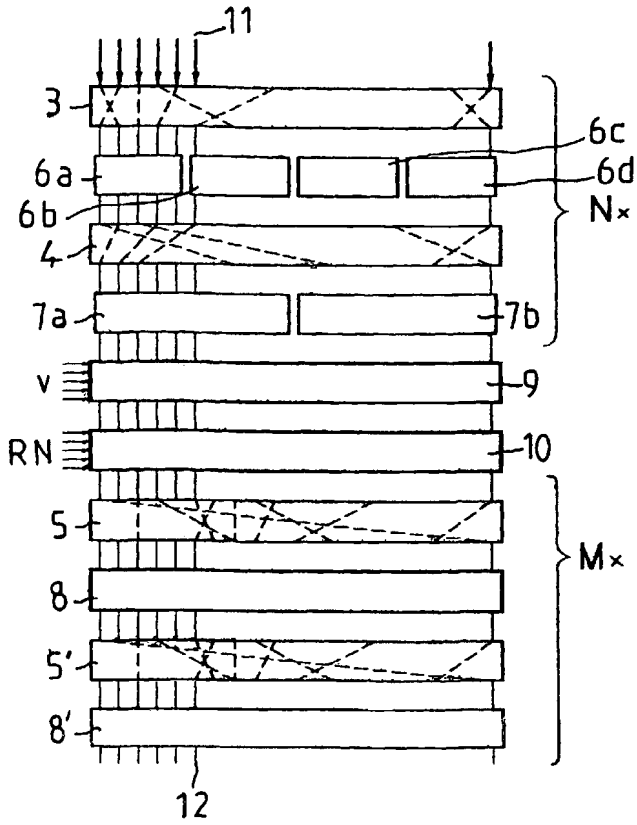
(74) Mandataires : **HAUTIER, Jean-Louis** etc.; Office Méditerranéen de Brevets d'Invention, et de Marques, Cabinet Hautier, 24, rue Masséna, F-06000 NICE (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE,

[Suite sur la page suivante]

(54) Title: METHOD AND DEVICE FOR ENCRYPTION OF DIGITAL DATA

(54) Titre : PROCEDE ET DISPOSITIF DE CHIFFREMENT DE DONNEES NUMERIQUES___



(57) Abstract: The invention concerns a method and a device for encryption of digital data. The device comprises an encryption string with means for permutation of data bits, means for substituting data bits and means for executing a XOR operation. The invention is characterized in that the permutation, substitution and logic operation means are hardware-implemented means.

(57) Abrégé : La présente invention concerne un procédé et un dispositif de chiffrement de données numériques. Le dispositif comporte une chaîne de chiffrement avec des moyens de permutation des bits de données, des moyens de substitution des bits de données et des moyens d'exécution d'une opération logique " ou exclusif ".Selon l'invention, les moyens de permutation, de substitution et d'exécution d'opérations logiques sont des moyens implémentés matériellement.

WO 03/092219 A1

SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **États désignés** *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

"Procédé et dispositif de chiffrement de données numériques"

La présente invention concerne un procédé et un dispositif de chiffrement de données numériques.

Elle trouvera particulièrement son application dans le domaine du chiffrement entre une mémoire à accès aléatoire (Random Access Memory, RAM) et un processeur.

Dans le domaine du cryptage en général, on connaît du document US-B1 6.320.964 un accélérateur cryptographique.

Cet accélérateur cryptographique comprend un sélecteur et une pluralité de bus couplée au sélecteur.

Certains des bus comprennent des moyens de réalisation d'une permutation de bits de données parmi d'autres opérations.

Ces autres opérations peuvent être des opérations « ou exclusif » ou des substitutions selon le principe général du standard DES (Data Encryption Standard).

Ce document reflète l'état de la technique général dans le domaine du chiffrement de données dans la mesure où il présente une combinaison de différents moyens de chiffrement et particulièrement des permutations, des substitutions et des opérations « ou exclusif » par le biais de moyens logiciels.

En effet, dans les systèmes cryptographiques actuels, l'implémentation est soit complètement logicielle soit une association de moyens logiciels et Hardware.

Ce type de système de chiffrement a l'inconvénient d'être lent ce qui pèse fortement sur certains échanges de données et particulièrement entre un processeur et une mémoire à accès aléatoire habituellement utilisée pour des échanges rapides.

Par ailleurs, les systèmes de chiffrement mis en œuvre selon l'art antérieur impliquent de nombreux échanges de données (notamment des clés) entre le processeur et la mémoire.

Cela pèse également sur la rapidité d'exécution de l'ensemble du processus de chiffrement.

La présente invention a pour objectif de proposer un procédé et un dispositif de chiffrement de données numériques qui permettent de ne pas handicaper la rapidité des échanges de données.

Pour ce faire, l'invention a l'avantage d'opérer un chiffrement de façon plus rapide.

En effet, son implantation strictement hardware assure une grande rapidité du chiffrement.

On notera que l'implémentation purement hardware du dispositif de chiffrement va à l'encontre d'un préjugé constant dans l'état de la technique selon lequel il est nécessaire de disposer d'une couche logicielle pour assurer un chiffrement avec une souplesse d'utilisation notamment quant à la saisie et les modifications de clés de chiffrement.

La présente invention a vaincu ce préjugé en proposant un nouveau dispositif et procédé de chiffrement implantés uniquement en hardware tout en assurant un chiffrement efficace des données.

Un autre avantage de l'invention est qu'elle ne nécessite que peu d'échanges avec le microprocesseur.

Un autre but de l'invention est de proposer un système de chiffrement particulièrement efficace et difficile à pirater.

D'autres buts et avantages apparaîtront au cours de la description qui suit d'un mode de réalisation préféré de l'invention qui n'est cependant qu'indicatif.

La présente invention concerne un dispositif de chiffrement de données numériques comportant une chaîne de chiffrement avec :

- des moyens de permutation des bits de données ;

- des moyens de substitution des bits de données ;

- des moyens d'exécution d'une opération logique « ou exclusif » caractérisé par le fait que lesdits moyens de permutation, de substitution et d'exécution sont des moyens implémentés matériellement.

Ce dispositif pourra se présenter suivant les modes de réalisation introduits ci-après :

- les moyens d'exécution d'une opération logique « ou exclusif » comportent au moins un moyen d'exécution situé vers le milieu de la chaîne de chiffrement ;

- les moyens d'exécution d'une opération logique « ou exclusif » comportent au moins une porte logique « ou exclusif » avec une entrée pour les données à chiffrer et une entrée pour une valeur fonction de l'adresse de stockage en mémoire de données à chiffrer ;

- la valeur fonction de l'adresse est l'adresse elle-même ;

- la valeur fonction de l'adresse est une partie de l'adresse obtenue par troncature ;

- la valeur fonction de l'adresse est obtenue par extension de l'adresse ;

- les moyens d'exécution d'une opération logique « ou exclusif » comportent au moins une porte logique « ou exclusif » avec une entrée pour les données à chiffrer et une entrée pour une valeur aléatoire ;

- la valeur aléatoire est modifiée à chaque remise à zéro du dispositif ;

- les moyens de substitution comportent des tables de substitution de données par paquets.

L'invention concerne également un procédé de chiffrement de données numériques comportant une chaîne d'étapes de chiffrement dans laquelle :

- on effectue des permutations des bits de données ;

- on effectue des substitutions des bits de données ;

- on exécute des opérations logiques « ou exclusif » caractérisé par le fait

qu'on effectue les étapes de chiffrement par utilisation de moyens implémentés matériellement.

Selon des variantes préférées, ce procédé comporte les étapes suivantes :

- on exécute au moins une opération logique « ou exclusif » vers le milieu des étapes de chiffrement ;
- on exécute au moins une opération logique « ou exclusif » par opération entre les données à chiffrer et une valeur fonction de l'adresse de stockage en mémoire des données à chiffrer ;
- on utilise comme valeur fonction de l'adresse l'adresse elle-même ;
- on obtient la valeur fonction de l'adresse en tronquant ladite adresse ;
- on obtient la valeur fonction de l'adresse par extension de l'adresse
- on exécute au moins une opération logique « ou exclusif » par opération entre les données à chiffrer et une valeur aléatoire ;
- on modifie la valeur aléatoire à chaque remise à zéro.
- on effectue au moins une substitution des bits de données par paquets de bits.

Les dessins ci-joints sont donnés à titre d'exemples et ne sont pas limitatifs de l'invention. Ils représentent seulement un mode de réalisation de l'invention et permettront de la comprendre aisément.

La figure 1 schématise l'utilisation préférentielle de l'invention pour un chiffrement de données entre un processeur et une mémoire à accès aléatoire.

La figure 2 illustre un mode de réalisation préféré du dispositif selon l'invention avec différentes étapes de chiffrement.

En référence à la figure 1, le dispositif et le procédé selon l'invention peuvent être mis en œuvre entre un processeur 1 et une mémoire du type à accès aléatoire 2 afin de chiffrer les données transmises par le bus de données 13.

Toute autre application à divers échanges de données n'est cependant pas exclue de la présente invention.

On a présenté en figure 2 un mode de réalisation préféré de l'invention pour le chiffrement de bits de données entrant 11.

Le repère 12 illustre les bits de données sortant issus du chiffrement.

En référence à cette figure, différents moyens de permutations 3, 4, 5 sont présents à différents niveaux de la chaîne de chiffrement.

Avantageusement, ces moyens de permutation 3, 4, 5 sont alternés avec d'autres moyens de chiffrement et particulièrement des moyens de substitution de bits de données 6a, 6b, 6c, 6d, 7a, 7b, 8.

Par ailleurs, des moyens d'exécution d'une opération logique « ou exclusif » sont également présents et représentés ici sous forme de portes logiques 9, 10.

A titre préféré, la chaîne de chiffrement s'organise comme suit : N x (alternances permutations/ Substitutions), XOR avec V, XOR avec RN (pas de permutations avec RN), M x alternances permutations / Substitutions), N et M >=1 de préférence au moins deux.

En référence à la figure 2, la chaîne de chiffrement peut débuter par une permutation 3 suivie d'une étape de substitution par les moyens 6a, 6b, 6c, 6d.

La substitution est opérée par des tables de substitution de données et préférentiellement réalisée par une pluralité de tables disposées en parallèle pour chiffrer des paquets distincts de bits de données.

Dans l'exemple de données échangées sur 16 bits, on pourra utiliser quatre tables de substitution de quatre bits.

On pourra également comme dans le cas des tables de substitution 7a, 7b utiliser deux tables de chiffrement de 8 bits.

Toujours en référence à la figure 2, on peut également constituer une table de substitution repérée 8 de 16 bits et réalisée de façon unique pour effectuer les tables de substitution de l'ensemble des bits de données.

Suite à des tables de substitution représentées aux repères 6a, 6b, 6c, 6d, on réalise une nouvelle permutation au niveau 4.

S'ensuit une nouvelle étape de substitution au niveau 7a, 7b.

On réalise alors une opération logique « ou exclusif » par l'intermédiaire de la porte 9.

On visualise clairement à la figure 2, que cette étape d'opération « ou exclusif » est positionnée sensiblement au milieu de la chaîne de chiffrement.

A titre préféré, on utilise pour l'opération logique « ou exclusif » une entrée d'une valeur fonction de l'adresse de stockage en mémoire des données à chiffrer.

Dans ce cadre, on a représenté par la lettre V une entrée de données représentative de l'adresse en mémoire.

A titre d'exemple, la valeur fonction de l'adresse peut être l'adresse elle-même, une valeur obtenue par troncature de l'adresse ou, plus généralement, une valeur obtenue par extension de l'adresse.

Cela dépendra de la longueur relative des données à chiffrer et de leur adresse.

Par extension on signifie que les bits de l'adresse sont recopiés et ou tronqués afin que la valeur obtenue comporte un même nombre de bits que la données avec laquelle on doit effectué un « ou exclusif ».

Suite à cette étape, on réalise une nouvelle étape d'opération logique « ou exclusif » repérée 10.

Au niveau de cette porte, une entrée est associée aux données à chiffrer et une autre entrée est associée à l'entrée d'un nombre aléatoire RN utilisé par la porte 10.

La réalisation d'une porte « ou exclusif » 10 avec une entrée d'une valeur aléatoire RN a l'avantage avec un faible surcoût et peu de perte de rapidité de gêner les attaques longues à base d'accumulation de résultats nécessitant beaucoup de traitement et donc parfois impliquant des remises à zéro.

Dans ce cadre, on changera avantageusement la valeur aléatoire RN à chaque remise à zéro du dispositif.

En ce qui concerne la porte « ou exclusif » 9, elle a également l'avantage de ne pas peser sur la rapidité du chiffrement et notamment en proposant des étapes de troncature ou d'extension de la valeur d'adresse pour l'adapter à la longueur des données de chiffrement qui sont des opérations techniquement rapides.

L'opération logique effectuée par la porte 10 peut être suivie d'une étape supplémentaire de permutation au repère 5 puis préférentiellement de substitution par la table 8.

Ces opérations 5, 8 peuvent être renouvelées M fois comme figuré.

En sortie, on obtient des données chiffrées repérées 12.

On réalise ainsi un chiffrement efficace c'est-à-dire difficile à percer tout en assurant une grande rapidité d'exécution des opérations de chiffrement.

On notera que dans le mode de réalisation préféré illustré, très peu d'échanges sont nécessaires entre le processeur et le dispositif de chiffrement notamment en ce qui concerne les paramètres de chiffrement.

En effet, l'ensemble du dispositif étant fixé au niveau matériel (implémentation hardware) les paramètres de chiffrement tels que des clés n'ont pas à être transmises par le microprocesseur.

En effet, son implantation strictement hardware assure une grande rapidité du chiffrement.

On notera que l'implémentation purement hardware du dispositif de chiffrement va à l'encontre d'un préjugé constant dans l'état de la technique selon lequel il est nécessaire de disposer d'une couche logicielle pour assurer un chiffrement avec une souplesse d'utilisation notamment quant à la saisie et les modifications de clés de chiffrement.

La présente invention a vaincu ce préjugé en proposant un nouveau dispositif et procédé de chiffrement implantés uniquement en hardware tout en assurant un chiffrement efficace des données.

REFERENCES

1. Processeur
2. Mémoire à accès aléatoire
3, 4, 5, 5'. Moyens de permutation
6a, 6b, 6c, 6d. Moyens de substitution
7a, 7b. Moyens de substitution
8, 8'. Moyens de substitution
9. Porte logique
10. Porte logique
11. Bits de données entrant
12. Bits de données sortant
13. Bus de données
V. Valeur
RN. Valeur aléatoire

REVENDICATIONS

1. Dispositif de chiffrement de données numériques comportant une chaîne de chiffrement avec :

- des moyens de permutation (3, 4, 5) des bits de données ;
- des moyens de substitution (6a,b,c,d, 7a, 7b, 8) des bits de données ;
- des moyens d'exécution d'une opération logique « ou exclusif » (9, 10)

lesdits moyens de permutation, de substitution et d'exécution étant des moyens implémentés matériellement,

caractérisé par le fait

que les moyens d'exécution d'une opération logique « ou exclusif » comportent au moins une porte logique « ou exclusif » (9) avec une entrée pour les données à chiffrer et une entrée pour une valeur (V) fonction de l'adresse de stockage en mémoire de données à chiffrer.

2. Dispositif selon la revendication 1, caractérisé par le fait

que les moyens d'exécution d'une opération logique « ou exclusif » comportent au moins un moyen d'exécution situé vers le milieu de la chaîne de chiffrement.

3. Dispositif selon l'une quelconque des revendications 1 ou 2 caractérisé par le fait

que la valeur (V) fonction de l'adresse est obtenue par extension de l'adresse.

4. Dispositif selon l'une quelconque des revendications 1 à 3, caractérisé par le fait

que les moyens d'exécution d'une opération logique « ou exclusif » comportent au moins une porte logique « ou exclusif » (10) avec une entrée pour les données à chiffrer et une entrée pour une valeur aléatoire (RN).

5. Dispositif selon la revendication 4, caractérisé par le fait

que la valeur aléatoire (RN) est modifiée à chaque remise à zéro du dispositif.

6. Dispositif selon l'une quelconque des revendications 1 à 5, caractérisé par le fait

que les moyens de substitution comportent des tables de substitution de données par paquets.

7. Procédé de chiffrement de données numériques comportant une chaîne d'étapes de chiffrement dans laquelle :

- on effectue des permutations (3,4,5) des bits de données ;
- on effectue des substitutions (6a,b,c,d, 7a, 7b, 8) des bits de données ;
- on exécute des opérations logiques ou « exclusif » (9, 10)
- on effectue les étapes de chiffrement par utilisation de moyens implémentés matériellement.

caractérisé par le fait

qu'on exécute au moins une opération logique « ou exclusif » par opération entre les données à chiffrer et une valeur fonction de l'adresse de stockage en mémoire des données à chiffrer.

8. Procédé selon la revendication 7, caractérisé par le fait

qu'on exécute au moins une opération logique « ou exclusif » vers le milieu des étapes de chiffrement.

9. Procédé selon la revendication 8, caractérisé par le fait

qu'on obtient la valeur fonction de l'adresse par extension de ladite adresse.

10. Procédé selon l'une quelconque des revendications 7 à 9, caractérisé par le fait

qu'on exécute au moins une opération logique « ou exclusif » par opération entre les données à chiffrer et une valeur aléatoire.

11. Procédé selon la revendication 10, caractérisé par le fait

qu'on modifie la valeur aléatoire à chaque remise à zéro.

12. Procédé selon l'une quelconque des revendications 8 à 11, caractérisé par le fait

qu'on effectue au moins une substitution des bits de données par paquets de bits.

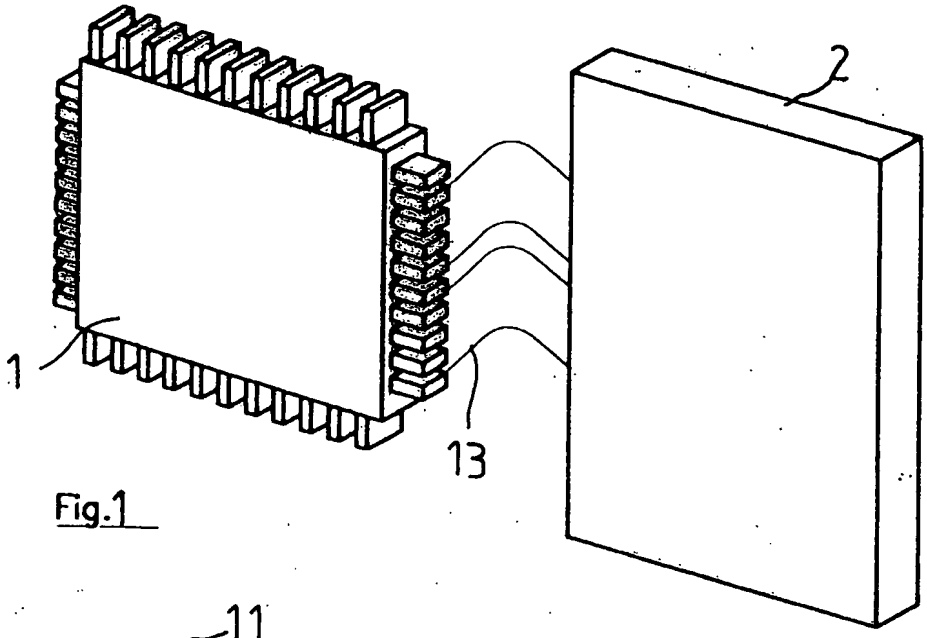


Fig.1

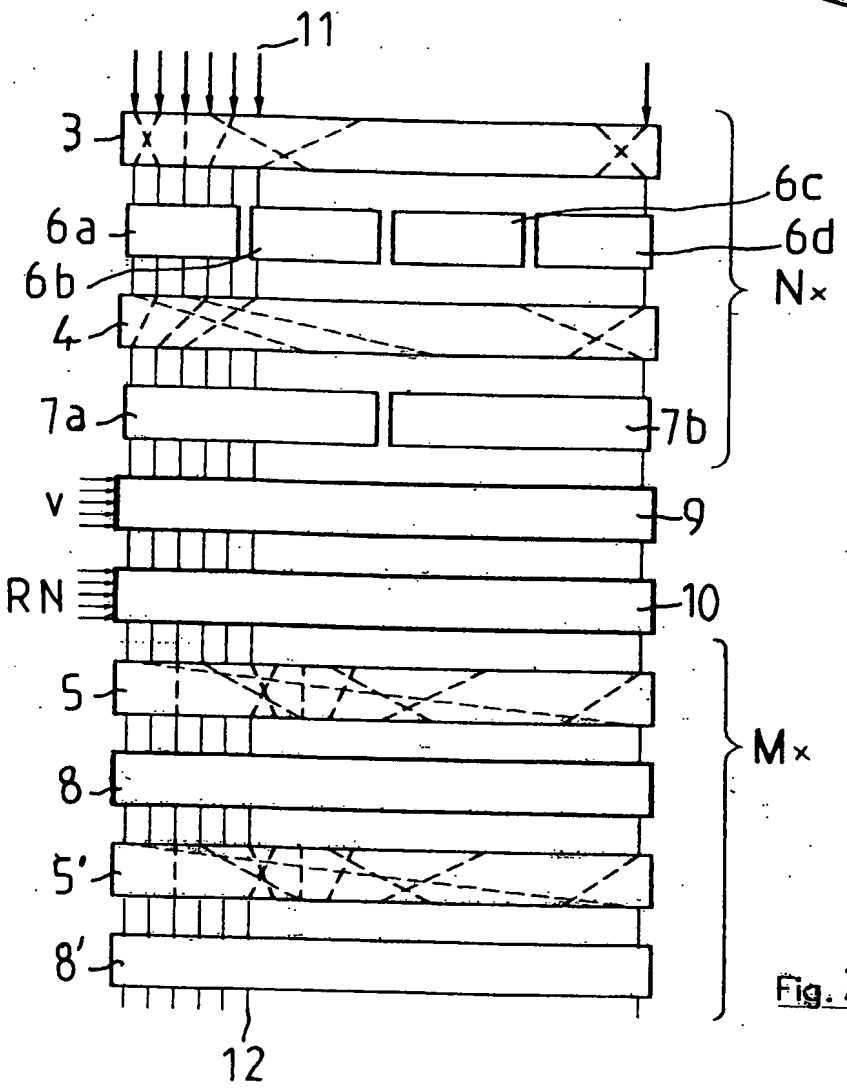


Fig. 2

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 03/01190

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 618 701 A (NIPPON ELECTRIC CO) 5 October 1994 (1994-10-05) abstract page 2, line 28 - line 37 page 4, line 50 -page 5, line 42	1,2,7,8
A	EP 0 802 653 A (VLSI TECHNOLOGY INC) 22 October 1997 (1997-10-22) column 3, line 2 - line 8 column 5, line 29 - line 48 column 6, line 53 - line 54	1,2,7,8

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 September 2003	19/09/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 03/01190

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0618701 A	05-10-1994	JP 2091220 C	18-09-1996
		JP 6266284 A	22-09-1994
		JP 8012537 B	07-02-1996
		AU 674197 B2	12-12-1996
		AU 5776494 A	15-09-1994
		CA 2118826 A1	12-09-1994
		DE 69429126 D1	03-01-2002
		DE 69429126 T2	11-07-2002
		EP 0618701 A2	05-10-1994
		US 5442705 A	15-08-1995
EP 0802653 A	22-10-1997	US 5835599 A	10-11-1998
		EP 0802653 A2	22-10-1997
		JP 10075240 A	17-03-1998

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 03/01190

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/06

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 618 701 A (NIPPON ELECTRIC CO) 5 octobre 1994 (1994-10-05) abrégé page 2, ligne 28 - ligne 37 page 4, ligne 50 -page 5, ligne 42	1,2,7,8
A	EP 0 802 653 A (VLSI TECHNOLOGY INC) 22 octobre 1997 (1997-10-22) colonne 3, ligne 2 - ligne 8 colonne 5, ligne 29 - ligne 48 colonne 6, ligne 53 - ligne 54	1,2,7,8

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
11 septembre 2003	19/09/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

1

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 03/01190

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0618701 A	05-10-1994	JP 2091220 C	18-09-1996
		JP 6266284 A	22-09-1994
		JP 8012537 B	07-02-1996
		AU 674197 B2	12-12-1996
		AU 5776494 A	15-09-1994
		CA 2118826 A1	12-09-1994
		DE 69429126 D1	03-01-2002
		DE 69429126 T2	11-07-2002
		EP 0618701 A2	05-10-1994
		US 5442705 A	15-08-1995
EP 0802653 A	22-10-1997	US 5835599 A	10-11-1998
		EP 0802653 A2	22-10-1997
		JP 10075240 A	17-03-1998